

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>	Application Number	09/394,143	
	Filing Date	September 10, 1999	
	First Named Inventor	Turgeon, Paul Charles	
	Art Unit	3621	
	Examiner Name	Calvin L. Hewitt II	
Total Number of Pages in This Submission		Attorney Docket Number	040048-000100US

ENCLOSURES (Check all that apply)		
<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/ Incomplete Application <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s)	<input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): Return Postcard
Remarks		The Commissioner is authorized to charge any additional fees to Deposit Account 2011480

RECEIVED
 APR 29 2003
GROUP 3600

RECEIVED
 2003 APR 23 AM 9:15
 BOARD OF PATENT APPEALS
 AND INTERFERENCES

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm or Individual	Townsend and Townsend and Crew LLP	
	Patrick M. Boucher	Reg. No. 44,037
Signature	<i>Patrick M. Boucher</i>	
Date	April 23, 2003	

CERTIFICATE OF MAILING		
Express Mail Label: EL 889382605 US		
I hereby certify that this correspondence is being deposited with the United States Postal Service with "Express Mail Post Office to Address" service under 37 CFR 1.10 on this date April 23, 2003 and is addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450		
Typed or printed name	Nina L. McNeill	
Signature	<i>Nina L. McNeill</i>	Date
		April 23, 2003

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

"Express Mail" Label No. EL 889382605US
Date of Deposit April 23, 2003

PATENT
Attorney Docket No.: 040048-000100US

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Address" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By: Nina L. McNeill
Nina L. McNeill

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of:

Paul Charles Turgeon

Application No.: 09/394,143

Filed: September 10, 1999

For: SYSTEM AND METHOD FOR
PROVIDING SECURE SERVICES
OVER PUBLIC AND PRIVATE
NETWORKS USING A REMOVABLE,
PORTABLE COMPUTER-READABLE
STORAGE MEDIUM AT A NETWORK
ACCESS DEVICE

Examiner: Calvin L. Hewitt II

Art Unit: 3621

APPELLANT BRIEF UNDER 37 CFR
§1.192

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

RECEIVED
2003 APR 28 AM 9:16
BOARD OF PATENT APPEALS
AND INTERFERENCES
RECEIVED
APR 29 2003
GROUP 3600

06/04/2003 PLEWIS 00000003 201430 09394143

01 FC:1402 320.00 CH
Appellant offers this Brief further to the Notice of Appeal mailed on
March 3, 2003. This Brief is submitted in triplicate as required by 37 CFR §1.192(a).

1. Real Parties in Interest

The real party in interest is NYCE Corporation.

2. Related Appeals and Interferences

No other appeals or interferences are known that will directly affect, are directly affected by, or have a bearing on the Board decision in this appeal.

3. Status of Claims

Claims 1 – 25 are currently pending in the application, which is a Continued Prosecution Application. All pending claims stand rejected by the Examiner. Claims 1, 2, 4 – 8, and 12 – 25 are as originally filed in the parent application on September 10, 1999; Claims 3 and 9 – 11 were amended in a response to the first Office Action that was filed on December 19, 2001. Original Claims 26 – 28 were canceled by Preliminary Amendment concurrently with filing the Continued Prosecution Application on September 13, 2002.

The rejections of Claims 1 – 25 are believed to be improper and are the subject of this appeal. Each of these claims has been rejected at least twice. A copy of Claims 1 – 25 as rejected is attached as an Appendix.

4. Status of Amendments

No amendments have been filed subsequent to the most recent rejection, mailed December 2, 2002.

5. Summary of the Invention

In one embodiment, the claimed invention relates to methods and systems for providing secure financial services over public communication lines, such as the Internet or other network (Application, p. 4, ll. 22 – 24). The secure financial services are provided by using encrypted information on a portable storage medium, such as a CD

(*id.*, p. 4, ll. 24). With this arrangement, the portable storage medium may effectively act as a debit card, allowing a customer holder of the portable storage medium to execute debit transactions electronically (*id.*, p. 4, ll. 24 – 26). The portable storage medium includes information that is typically found on the magnetic strip of conventional plastic debit card, such as the customer's name, account routing number, and the like (*id.*, p. 4, l. 26 – p. 5, l. 2).

While the information from the magnetic-strip of a conventional debit card is readable by any magnetic-strip reader, the information is encrypted on the portable storage medium of the invention (*id.*, p. 5, l. 23 – 25). The holders of such portable storage media are assigned an electronic PIN that may be used in accordance with embodiments of the invention to resolve the conventional PIN used in debit transactions (*id.*, p. 6, ll. 1 – 3). In this way, the card information may remain secure even when transmitted over the Internet or other network (*id.*, p. 6, ll. 14 – 15). This differs from a conventional debit card, whose security relies primarily on the security of the card itself and the conventional PIN, reflecting the fact that conventional debit transactions are not subject to potential interception over public communication lines. In addition to this encrypted information, the portable storage media may include personalized unencrypted information used in providing a greeting, advertising, and the like to the customer when the electronic debit card is used (*id.*, p. 12, ll. 16 – 20).

Use of these methods and systems is illustrated in the application with the example of an Internet debit transaction conducted at a merchant web site, although there may be other uses. In such a transaction, the customer may make payment by inserting the portable storage medium into a network access device, *e.g.* by inserting the electronic debit card into a CD drive of a personal computer, and entering his electronic PIN (*id.*, p. 6, ll. 23 – 24). The encrypted information is transmitted with the electronic PIN to a module on the merchant's web site (*id.*, p. 6, ll. 25 – 26). This module establishes a secure connection with a decryption interface, which forwards a *re*-encrypted PIN to a financial institution to seek an approval or denial code (*id.*, p. 7, ll. 2 – 7). This backend seeking of an approval code may be similar to a traditional debit transaction using an

existing secure financial network (*id.*, p. 13, l. 23 – p. 14, l. 1) so that, if approved, funds are debited directly from the customer's account (*id.*, p. 14, ll. 3 – 5). The transaction at the merchant web site may be completed (or not) when the approval (or denial) code is returned to that site (*id.*, p. 14, l. 17 – p. 15, l. 5).

6. Issues

Issue 1: Whether under 35 U.S.C. §103(a) Claims 1 – 9, 12 – 20, and 23 – 25 are unpatentable over U.S. Pat. No. 5,903,881 issued to Schrader *et al.* (hereinafter “Schrader”) in view of U.S. Pat. No. 5,457,746 issued to Dolphin (hereinafter “Dolphin”). Section 5 beginning on page 3 of the Office Action mailed December 2, 2002 (paper no. 20, hereinafter “the Office Action”) describes the Examiner's position on this issue, supplemented by remarks in Section 3 beginning on page 2 of the Office Action.

Issue 2: Whether under 35 U.S.C. §103(a) Claims 10, 11, 21, and 22 are unpatentable over Schrader in view of U.S. Pat. No. 5,913,202 issued to Motoyama (hereinafter “Motoyama”) and U.S. Pat. No. 6,195,357 issued to Polcyn (hereinafter “Polcyn”). Section 5¹ beginning on page 7 of the Office Action describes the Examiner's position on this issue.

7. Grouping of the Claims

For purposes of this appeal, the claims are grouped as follows. Groups 1 and 2 pertain to Issue 1 and Group 3 pertains to Issue 2.

Group 1: Claims 1 – 4, 9, 12 – 20, and 23 – 25.

¹There is a misnumbering in the Office Action so that two sections “5” are identified, one beginning on page 3 and the other beginning on page 7.

Group 2: Claim 5 – 8.

Group 3: Claims 10, 11, 21, and 22.

Although certain claims are grouped above, Appellant reserves the right outside the context of this appeal to argue independent patentability of any grouped claims.

8. Argument

I. Issue 1: Patentability of Claims 1 – 9, 12 – 20, and 23 – 25

Each of Claims 1 – 9, 12 – 20, and 23 – 25 stands rejected under 35 U.S.C. §103(a) as unpatentable over Schrader in view of Dolphin.

In addressing the rejections of these claims below, it is useful as an initial matter, to discuss the disclosures of Schrader and Dolphin since this highlights how strikingly different they are in conceptual scope from what Appellant claims.

Schrader discloses a personal online banking system. This system is embodied in a software product that allows a user of a personal computer to perform a variety of banking activities, such as account management, bill payment, and balance determination (Schrader, Col. 5, l. 65 – Col. 6, l. 12). To the extent Schrader discusses the use of a computer-readable *portable* storage medium, such as a CD-ROM, it does so in the context of a delivery mechanism for the software product, noting that the software application is installed from that delivery mechanism onto the user's computer (*id.*, Col. 12, ll. 62 – 67) — in effect, like most software products, a CD-ROM is provided in the box purchased by the customer, used to install the software on his PC, and then stored away. Nothing in Schrader suggests anything other than the perfectly normal use of the installed software product on the user's PC after it has been installed, without further need of the delivery mechanism.

Dolphin discloses a mechanism for controlling distribution of periodicals. Multiple periodicals are encrypted onto CD-ROMs (Dolphin, Col. 4, ll. 12 – 18), which are then distributed to customers (*id.*, Col. 4, ll. 26 – 32). In addition to this encrypted information, some unencrypted information is included on the CD-ROM to permit access to menus of the content of the CD-ROM (*id.*, Col. 4, ll. 39 – 44). The user may then establish a connection with a billing/access center to download a code for decrypting those portions for which he wants to pay for access (*id.*, Col. 4, ll. 48 – 54). As part of an auditing function, a PCMCIA card installed on the user's PC maintains a log accessible by the billing/access center to monitor access of the periodicals (*id.*, Col. 11, ll. 25 – 28). Such monitoring is described as permitting the billing/access center to provide publishers of the periodicals with such auditing data as the number of times specific publications are viewed (*id.*, Col. 11, ll. 28 – 30).

1. Group 1: Claims 1, 12 – 20, and 23 – 25

To support a rejection under 35 U.S.C. §103, the Examiner is charged with factually supporting a *prima facie* case of obviousness. Manual of Patent Examining Procedure, Eighth Edition, First Revision, February, 2003 (hereinafter "MPEP") 2142. Such a *prima facie* case requires, *inter alia*, that all limitations of the claims be taught or suggested by the cited reference(s) and that there be some suggestion or motivation to combine or modify the reference teachings as the Examiner proposes. MPEP 2143. The rejections of the claims of Group 1 are deficient in at least both these respects.

The claims of Group 1 include the two pending independent claims, Claims 1 and 17, which respectively recite a system and method for providing financial services over a public network. The limitations of these claims require, *inter alia*, that "a customer us[e] ... a computer-readable portable storage medium to access a customer's financial account via [a] public network" and that "a financial institution ... determine[] an access to said customer's financial account on the basis of the [information decrypted from the portable storage medium]." These limitations are simply not taught or

suggested by either Schrader or Dolphin. In particular, the Examiner has explicitly conceded that Schrader does not disclose retrieving encrypted information from the computer-readable storage medium (Office Action, p. 5, "However, Schrader et al. do not teach of encrypted data stored on a CDROM."). Instead, the Examiner relies exclusively on Dolphin for these limitations (*id.*, p. 5), which Appellant previously emphasized fails to disclose doing anything with the encrypted periodical information other than decrypting it for the user to read (Preliminary Amendment filed September 13, 2002, p. 8).

In response to this argument, the Examiner has now pointed to the auditing functions that are disclosed in Dolphin as permitting the billing/access center to monitor and notify publishers of accessed periodicals with information such as the number of times they are accessed (Office Action, p. 2). The Examiner incorrectly deduces that

[t]herefore, in order to accurately bill and audit a customer, a direct correlation must exist between the user, user account and the decrypted data accessed, hence Dolphin clearly teaches "...encrypted information retrieved from a computer-readable storage medium to be used in determining access to a customer's financial account."
(Office Action, pp. 2 – 3).

This conclusion reflects an erroneous reading of Dolphin. The "auditing" functions that Dolphin describes relate merely to collecting and/or reporting to publishers information about frequency of access (Dolphin, Col. 11, ll. 27 – 30). There is nothing in Dolphin to suggest that the amount to be billed to the customer is dependent on this frequency. Even if it did, there is no reason why access to a customer's financial account would be dependent on *information decrypted from the portable-storage medium* as the claims require. To wit, in Dolphin, the content of the decrypted periodical is completely irrelevant to the billing/access center's access to a customer's financial account.

In addition, Appellant notes that there is no basis, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine Schrader and Dolphin in the manner suggested by the Examiner. *See* MPEP

2143. Appellant previously noted that the Examiner seems improperly to suggest that the level of skill in the art is being relied upon for such a motivation (*see* Preliminary Amendment filed September 13, 2002, pp. 8 – 9), but the Examiner has not responded to this basis for traversal of his rejection.

In any event, Appellant is unable to discern any suggestion in Schrader that its online banking system could be combined with the publication-distribution system of Dolphin, nor any suggestion in Dolphin that its publication-distribution system could be combined with the online banking software of Schrader; furthermore, the Examiner has failed to point to any such suggestion as required to establish a *prima facie* case. MPEP 2143. Even if Schrader and Dolphin were combined, their combination would not result in the claimed invention. At best, the combination of Schrader and Dolphin would teach providing multiple encrypted software products on a CD ROM, one of which is online banking software, and providing access keys to particular software products based on which ones a purchaser has paid for. Nothing in Schrader, Dolphin, or their combination teaches or suggests using information encrypted on the CD ROM in the manner required by the claims.

2. Group 2: Claims 5 – 8

Each of the claims in Group 2 depends from Claim 1. Accordingly, the arguments set forth with respect to Group 1, namely that some limitations are not disclosed in any of the cited art and that there is no motivation to combine the cited art as the Examiner suggests, are equally applicable to this group of claims.

Furthermore, each of the claims of Group 2 also requires, beyond the limitations of the claims of Group 1, that the decryption processor be “operative to extract a second identifier pertaining to said customer’s financial account from the decrypted information and to re-encrypt the extracted second identifier.” This second identifier is in addition to a first identifier related to the customer’s financial account requested from the customer. Neither Schrader nor Dolphin discloses these additional

limitations. Specifically, there is no disclosure of requiring *two* identifiers for access to the financial account, one of which is extracted from the decrypted information and then *re-encrypted*. The Examiner cites large passages of Schrader in support of this aspect of the rejection (Office Action, p. 4, *citing* Schrader, Fig. 15; Col. 15, ll. 5 – 55; Col. 16, l. 63 – Col. 17, l. 45; and Col. 18, l. 58 – Col. 19, 24), identifying the second identifier as an “account number”. (Office Action, p. 4) Notwithstanding the length of these passages, they plainly fail to disclose a second identifier extracted from information decrypted from the portable storage medium and then re-encrypted.

In fact, the only discussion of “account number” in Schrader occurs in the sections titled “Registration” (Schrader, Col. 15, ll. 27 – 54) and “Bill Payment” (*id.*, Col. 15, l. 55 – Col. 16, l. 21), and of these, the Examiner relies only on the “Registration” section. In its entirety, that section reads as follows:

In a preferred embodiment, the personal online finance application 304 enables the user to enter account information for a number of financial institutions and payees in order to register the user's account for later transactions. For each financial institution, the account information includes an account number, an account type which could be one of checking, savings, money market, line of credit and credit card, an account description, and the financial institution's routing number. The user also enters a social security number. Checking accounts and money market accounts may additionally be enabled for bill payment, which will allow users to write electronic checks from these accounts. Account creation is handled internally by the database module 1407, which modifies the transaction database to include additional accounts using the registration information.

Once the accounts have been registered, the user may create transactions in these accounts. Account information may be modified at any time, but this will affect all existing transactions that are related to that account. New accounts may be added or accounts may be deleted when necessary. The user may also enter a list of payees to whom the user intends to make payments. Each payee is characterized by a name, an account number, an address, and a telephone number. Payee information is stored with each account separately in the transaction database.
(Schrader, Col. 15, ll. 27 – 54).

This section merely reflects the fact that account-number information may be provided when using the online banking software of Schrader. Even acknowledging that this information may be encrypted when transmitted (*id.*, Col. 17, ll. 12 – 15), there is no suggestion whatsoever that it be “extracted[ed from] the decrypted information and ... re-encrypt[ed]” as the claims require.

The “Bill Payment” section of Schrader adds nothing pertinent. In that discussion, it is merely noted that fields may be completed, some of which include specification of an account number, when preparing information to effect a bill payment with the online banking software (*id.*, Col. 15, ll. 61 – 64). Nothing suggests that the account number act as a second identifier that is decrypted from the portable storage medium and then re-encrypted.

For this additional reason, the claims of Group 2 are also believed to be patentable.

II. Issue 2 (Group 3): Patentability of Claims 10, 11, 21, and 22

Each of Claims 10, 11, 21, and 22 stands rejected under 35 U.S.C. §103(a) as unpatentable over Schrader in view of Motoyama and Polcyn. Each of these claims is believed to be patentable by virtue of its dependence from either Claim 1 or Claim 17, the reasons for the patentability of both of which were discussed above.

In order for the rejection to be maintained under 35 U.S.C. §103 all limitations of the claims must be taught or suggested by the cited reference(s) and there must be some suggestion or motivation to combine or modify the reference teachings as the Examiner proposes. MPEP 2143. In this context, Appellant notes that the Examiner has not relied on Dolphin for the rejection of these claims, and has also conceded that Schrader does not disclose retrieving encrypted information from the computer-readable storage medium, a limitation embodied by all the claims of Group 3 by virtue of their dependencies (Office Action, p. 5, “However, Schrader et al. do not teach of encrypted data stored on a CDROM.”). The Office Action fails to address how this limitation is disclosed in Motoyama or Polcyn, and is for that reason alone defective. *In Re Royka*, 180 USPQ 580 (CCPA 1974).

In this respect, Appellant further notes that the Examiner also does not address any of the limitations in the claims intermediate in dependence between the claims of Group 3 and the base independent claims. Claims in dependent form are to be


construed to include all the limitations of the claim incorporated by reference into them.
37 C.F.R. §1.75. Since no art has been cited for these other limitations, the claims of
Group 3 are also valid for this additional reason.

The failure of the Office Action to address many of the limitations embodied by the claims of Group 3 makes plain that it is improper, and Appellant is highly reluctant to surmise an alternative basis that the Examiner may have had in mind for rejection of those claims. Appellant merely notes that a rejection that additionally applied Dolphin would appear to suffer from the same deficiencies as discussed above in connection with Group 1.

9. Conclusion

Appellant believes that the above discussion is fully responsive to all grounds of rejection set forth in the application. Please deduct the requisite fee of \$320.00 pursuant to 37 C.F.R. §1.17(c) from Deposit Account 20-1430 and any additional fees that may be due in association with the filing of this Brief.

Respectfully submitted,


Patrick M. Boucher
Reg. No. 44,037

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
PMB:pmb
DE 7101000 v1

APPENDIX

The claims pending in the application are as follows:

1. (Original) A system for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said system comprising:

a network access device including a programmable controller for executing code and a memory for storing a browser software to interface with said public network, a customer using said network access device and a computer-readable portable storage medium to access a customer's financial account via said public network, said computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account; and

a decryption processor, connected to said network access device via said public network, for decrypting said encrypted information retrieved from said storage medium such that a financial institution, connected to said decryption processor via said private network, determines an access to said customer's financial account on the basis of the decrypted information.

2. (Original) The system according to Claim 1, further comprising a computer connected to said network access device via said public network, said computer hosting a site for goods or services available on-line, said computer comprising a microprocessor being operative to transfer an active module to said network access device in response to said customer requesting the access to said customer's financial account by using said computer-readable portable storage medium.

3. (Previously Amended) The system according to Claim 2, wherein said active module contains code which is executed by said programmable controller in said network access device such that at least part of said unencrypted information is provided to said customer who is requested to enter a first identifier related to said customer's financial account.

4. (Original) The system according to Claim 3, wherein said programmable controller is operative to transfer the entered first identifier and the encrypted information to said computer for forwarding to said decryption processor.

5. (Original) The system according to Claim 4, wherein said decryption processor is operative to extract a second identifier pertaining to said customer's financial account from the decrypted information and to re-encrypt the extracted second identifier.

6. (Original) The system according to Claim 5, further comprising a network switch located on said private network for routing the re-encrypted second identifier received from said decryption processor to said financial institution maintaining said customer's financial account for determining whether to approve the access to said customer's financial account.

7. (Original) The system according to Claim 6, wherein said financial institution generates a code for indicating whether or not the access to said customer's financial account has been approved and transfers the generated code to said decryption processor via said network switch.

8. (Original) The system according to Claim 7, wherein customer's address data is displayed to said customer on said network access device if said code represents an access approval.

9. (Previously Amended) The system according to Claim 3, wherein the provided unencrypted information includes a name of said financial institution maintaining said customer's financial account.

10. (Previously Amended) The system according to Claim 3, wherein the provided unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

11. (Previously Amended) The system according to Claim 3, wherein the provided unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

12. (Original) The system according to Claim 1, wherein said computer-readable portable storage medium is a CD-ROM.

13. (Original) The system according to Claim 12, wherein said CD-ROM is produced by a card production facility, based on a card production file, for mailing said CD-ROM to said customer.

14. (Original) The system according to Claim 13, wherein said card production file includes an encrypted first identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

15. (Original) The system according to Claim 14, wherein said encrypted first identifier is generated by an encryption module for encrypting a first identifier.

16. (Original) The system according to Claim 15, wherein said first identifier prior to the encryption is generated by a card issuance system which is further operative to generate a second identifier pertaining to said customer's financial account, the generated second identifier being transferred to a mailer production facility for mailing to said customer.

17. (Original) A method for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said method comprising:

accessing a customer's financial account via said public network using a network access device and a computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account;

retrieving said encrypted and unencrypted information from said storage medium; and decrypting the retrieved encrypted information such that a financial institution determines an access to said customer's financial account on the basis of the decrypted information.

18. (Original) The method according to Claim 17, further comprising using said computer-readable portable storage medium in said network access device in response to an active module being downloaded to and executed at said network access device such that said unencrypted information is displayed to said customer.

19. (Original) The method according to Claim 18, further comprising entering an identifier pertaining to said customer's financial account in response to the executed active module.

20. (Original) The method according to Claim 19, wherein said unencrypted information includes a name of said financial institution maintaining said customer's financial account.

21. (Original) The method according to Claim 19, wherein said unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

22. (Original) The method according to Claim 19, wherein said unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

23. (Original) The method according to Claim 17, wherein said computer-readable portable storage medium is a CD-ROM.

24. (Original) The method according to Claim 23, wherein said CD-ROM is produced on the basis of a card production file that includes an encrypted identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

25. (Original) The method according to Claim 17, further comprising reviewing customer's address data displayed on a monitor of said network access device if said financial institution has approved the access to said customer's financial account.